Crypta

File Security Programme

User's manual

Copyright © 2010-2013 Česká pošta, s.p. and ICZ a.s.

No part of this document may be copied in any way whatsoever without the written consent of the copyright owners.

Copyrighted and other works derived from this work are subject to the owners' copyright protection.

Certain names of products and companies quoted in this work may be trade marks of the relevant owners.

Content

Chapter 1. Introduction 4
1.1. Standards 5
1.2. Profile 5
Chapter 2. System requirements and file sizes 5
2.1. System requirements 5
2.2. Maximum size of processed files 6
3.1. Installation progress - with graphical interface 6
Chapter 4. Programme functions - without selected profile 9
4.1. Programme launch 9
4.2. Application setting 10
4.3. Ending programme 12
4.4. Adding profile 12
4.5. Partners directory 14
4.6. Import of certificate 15
4.7. Update CRL 15
4.8. Error ouput 16
4.9. Decrypt 16
4.10. Verify signature 17
4.11. Profile login 18
Chapter 5. Programme functions - with selected profile 18
5.1. Edit profile 19
5.2.Generation of certificate application form 20
5.4. Import pair of keys / PKCS#12 21
5.5. Export certificate and certificate including private key/PKCS#12 21
5.6. Warning of upcoming certificate expiry 22
5.7. Certificate renewal 23
5.8. File signing 24
5.9. File signing and encrypting 25
Chapter 6. Unistallation 26
Appendix A. Command line interface 27
1. Verification of certificates against CRLs in the command line regime 27
2. Download CRL 27

3. Copy CRL 27
4. Encryption 28
5. Signing 28
9. Decryption 28
10. Archiving services, ... 28
11. Save password as file 28
12. Certificate database content summary 29
13. Update recipient 29
14. Check certificate status and validity 29
Appendix B. Application programme interface (API) 29

Chapter 1. Introduction

Crypta is a special programme intended for Czech Post's customers who need to transfer data to the Post for services such as SIPO or for payment system in a secured manner, i.e. with attached guaranteed electronic signature and encrypted. The programme is a newer version of the previous Crypta application, latest version 1.3, and works in a similar way. Crypta compresses the data into a ZIP file and secures the file with electronic signature and the right encryption for the specific task of Czech Post. Such output file is then transferred by the customer in a normal way to the relevant office of Czech Post. This communication is not ensured by Crypta. The recipient of the secured file will then use Crypta to decrypt the file and verify the electronic signature. This ensures

- confidentiality,
- integrity, and
- undeniability

of the transferred data.

The design of Crypta complies with the current practice of the relationship between Czech Post and its customers. Each Czech Post's task has its own certificate for file encryption. Customers are identified separately in individual Czech Post's tasks, i.e. they have a separate certificate with a different identification name for each task. However, encryption certificates and signature are not separated.

Crypta works exclusively with certificates issued by Czech Post's Public Certification Authority PostSignum. Certificates issued by Czech Post's Internal Authority are no longer acceptable. The validity of certificates is checked against the current Certificate Revocation Lists (CRLs).

Crypta is written in the programming language Java version 1.6; as such it can be run on all platforms which support the Java runtime environment of this or a higher version. Crypta uses the IAIK cryptography library for its cryptographic functions.

Crypta can be called both manually through the graphical interface or from other applications from the command line interface or via the application programme interface (API).

The software is supplied with a comfortable installation programme. If a new version is launched, it will be possible to update the Crypta software via the Czech Post's updates website PowerUpdate.

Crypta does not process files created in the previous Crypta version 1.3 for the Windows OS. Back compatibility is ensured only to the extent of recognition of a previous format.

1.1. Standards

File format

Crypta is used for secured file formats according to standard PKCS#7 (CMS) - SignedData and EnvelopedData. Its compatibility with Crypta version 1.3 is restricted to the extent that it recognises the previous file format and informs the user accordingly.

Public key certificates

The application supports certificates according to standard X.509 v.3.

Key storage

Keys and certificates are stored in files according to standard PKCS#12.

Electronic signature

The programme creates electronic signatures according to RSA SHA256.

Encryption

Algorithm AES256 or optionally AES128 in the CBC mode are used for encryption. Depending on the selected option, a key of the right size and a random 128-bit initialization vector are generated.

1.2. Profile

As already mentioned, the programme respects the current practice of setting certificates for individual tasks and customers and of introducing so-called profiles (similarly to Crypta 1.3 where this setting is called user profile). A profile is a specific programme setting in which one defined signature and encryption customer certificate is selected and in which communication with one selected Czech Post's task is expected. As already mentioned, certificates are not separated from encryption and signature keys.

Non-public data in the profile is protected with a password which is common to all users. All users introduced in the relevant operating system have the same access to the given profile. Any restrictions require the use of the operating system functions.

Chapter 2. System requirements and file sizes

2.1. System requirements

The application is intended for the Windows XP, Windows Vista and Windows 7, Windows Server 2003 and 2008, Solaris, AIX and Linux operating systems. The installation package for the above-mentioned operating systems includes Java 2 Runtime Environment (JRE) version 1.6. It is recommended to use the runtime environment from the installation package.

Encryption policies: The runtime environment JRE installed from a CD includes a setting for Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. If you chose another JRE to run Crypta, download the relevant encryption policies from the Java website. Note: The programme will not work without this arrangement.

The workstation HW configuration largely depends on the size of processed files.

Recommended configuration: Pentium IV 3 GHz, 1 GB RAM, 100 MB disk space, CD-ROM drive, mouse or another cursor positioning device, minimum monitor resolution 1024x768.

2.2. Maximum size of processed files

The maximum size of processed files depends on the size of the memory allocated for the Java runtime environment. The implicitly allocated memory is 256 MB, which is enough for the processing of file sized up to about 60 MB. (This approximate size refers to a file whose size will not be significantly reduced by compression.) For larger files it is recommended to set a larger memory size. The setting is done

- for graphical environment, in the file Crypta.vmoptions,
- for the command prompt, in the file CryptaCmd.vmoptions

in the installation directory of the application. It is necessary to set the Java activation parameter value to, e.g. -Xmx512m, or to another adequate value according to the HW configuration.

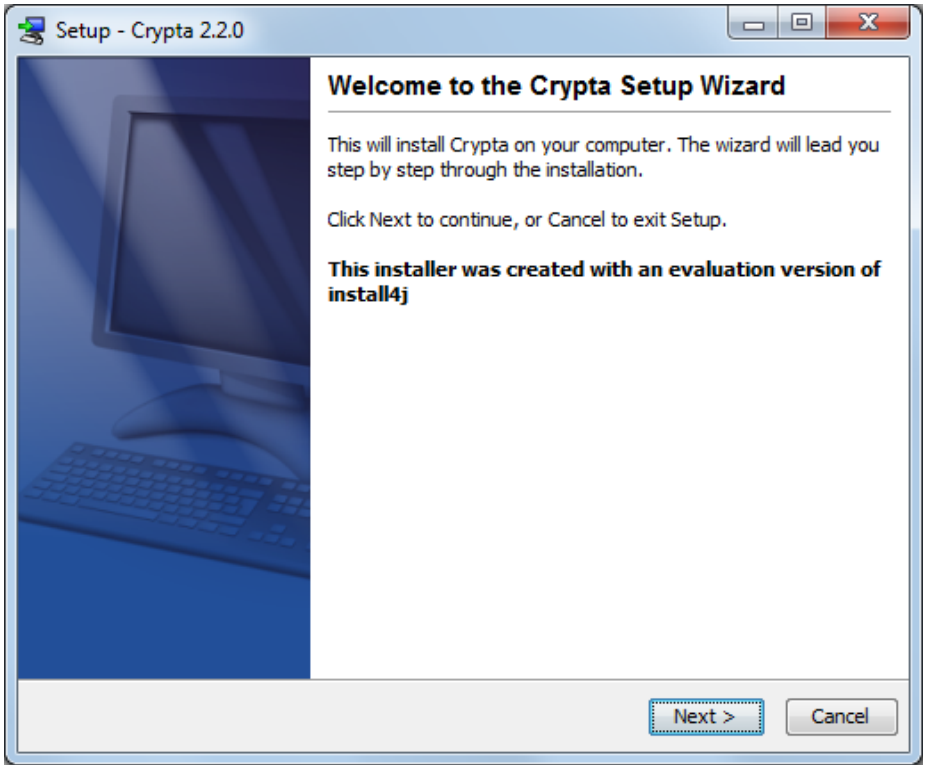
Chapter 3. Installation

3.1. Installation progress - with graphical interface

The following pictures demonstrate the programme installation progress.

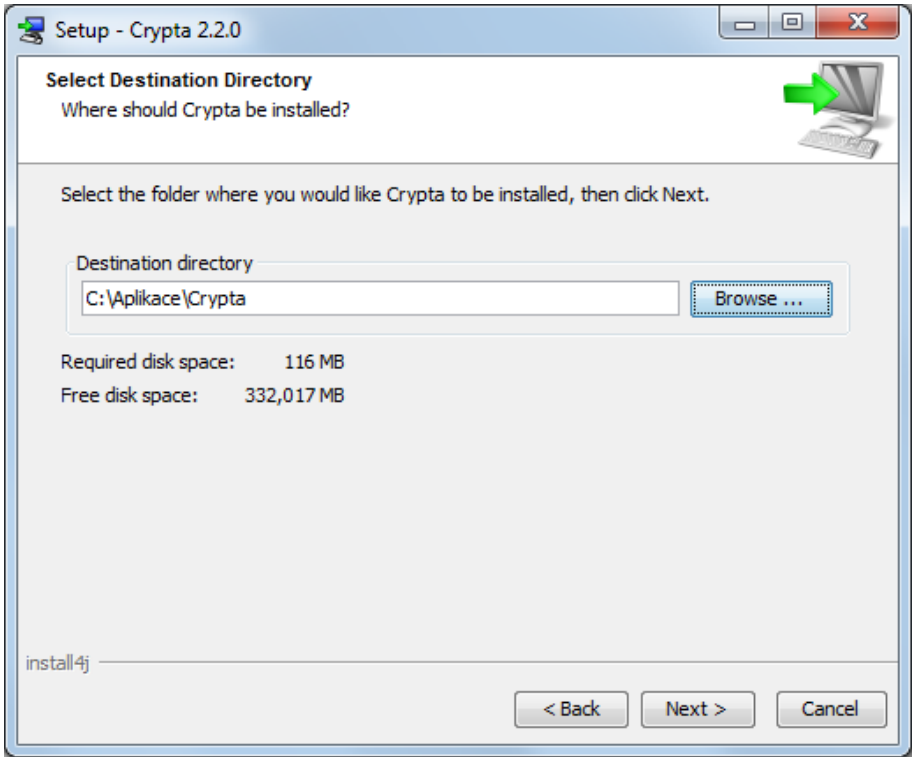
The opening panel follows. During the installation process it is recommended to close the other programmes. The Next button takes you to the next installation step, the Back button can be used to return back to previous dialogues for change of settings. The Cancel button allows you to discontinue the installer.

Picture 3.1. Opening panel

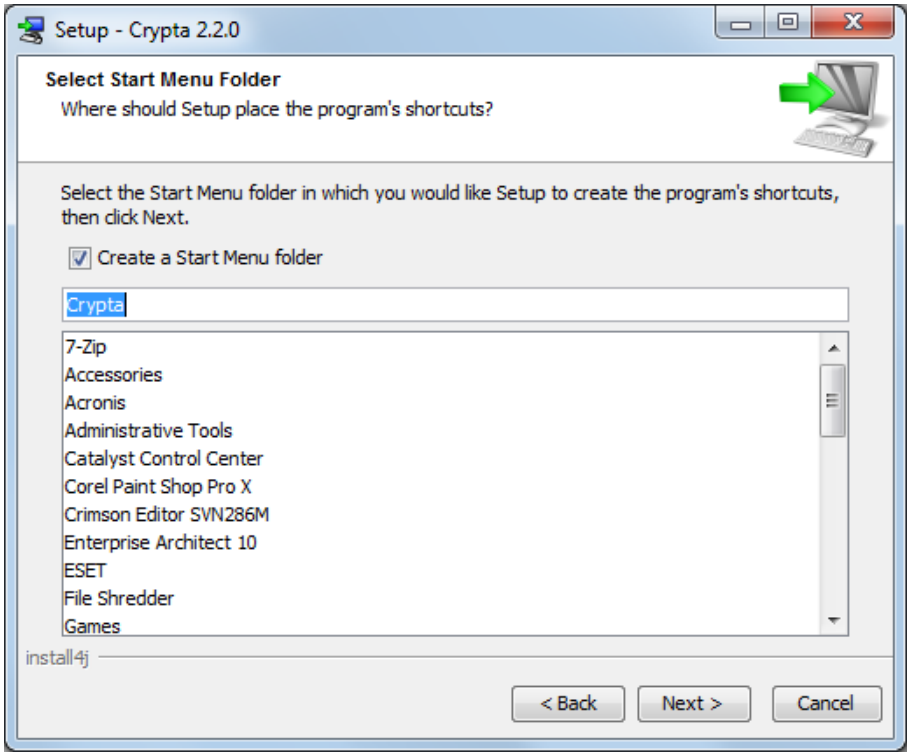

Setup - Crypta 2.2.0
Welcome to the Crypta Setup Wizard
This will install Crypta on your computer. The wizard will lead you step by step through the installation.
Click Next to continue, or Cancel to exit Setup.
This installer was created with an evaluation version of install4j
Next >
Cancel

The next dialogues are used to select the directory in which Crypta will be installed and to set the application shortcut. It is recommended to select an installation directory other than Program Files because you may need to edit the configuration files.

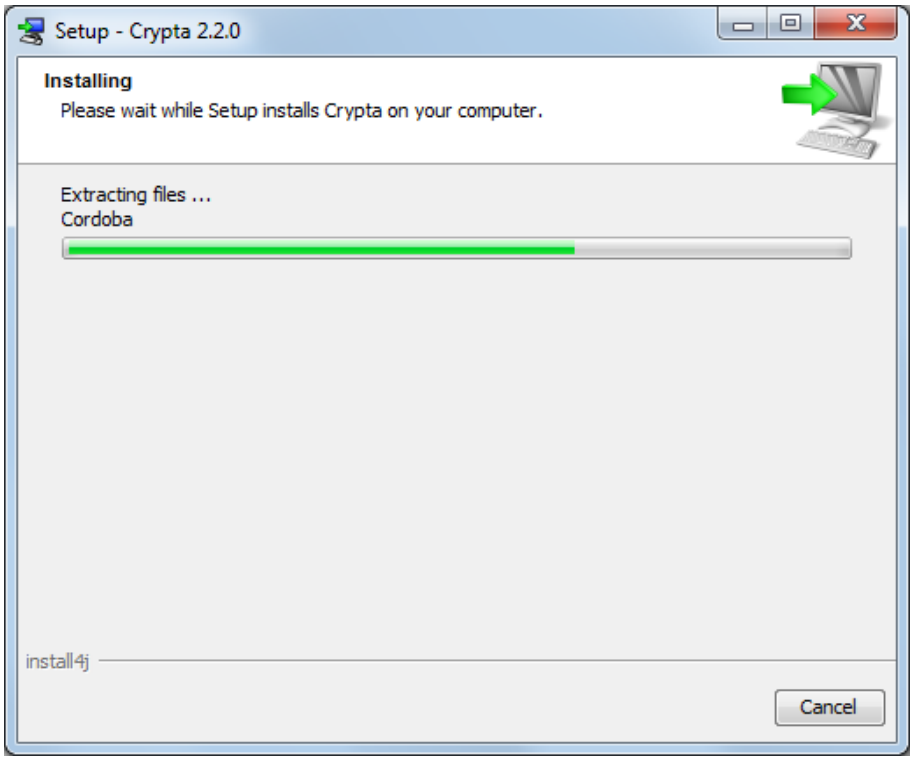
Picture 3.2. Installation directory selection



Picture 3.3. Shortcut file selection

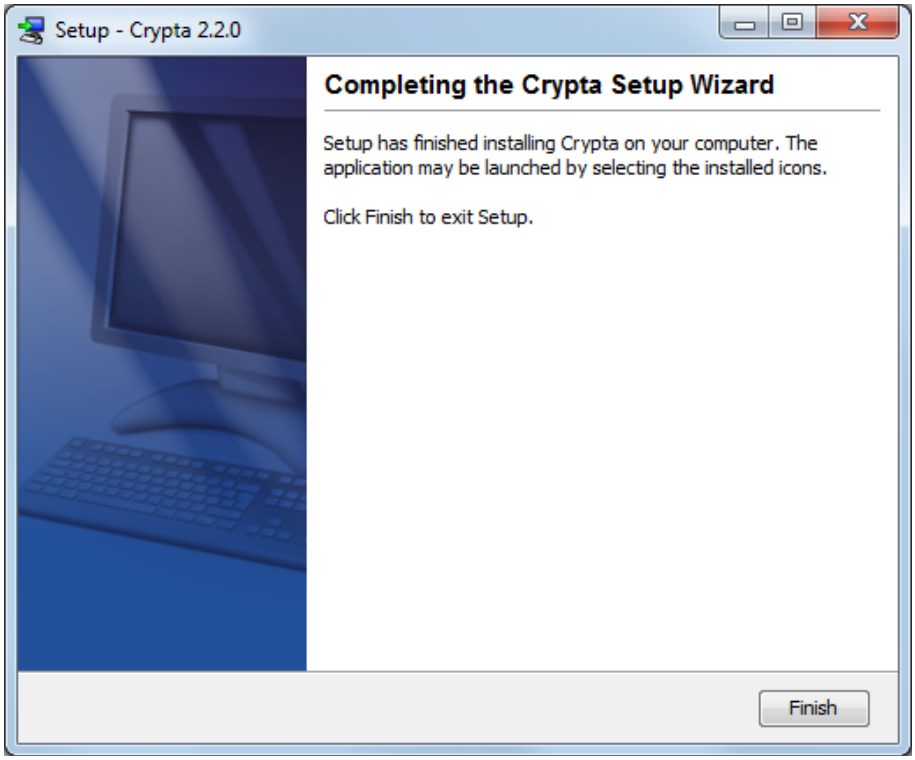


Picture 3.4. Installation progress



You will be informed about the progress and successful completion of the installation, or about any problem which may have occurred during installation. You can still use the Cancel button during the installation.

Picture 3.5. Installation completion


Setup - Crypta 2.2.0
Completing the Crypta Setup Wizard
Setup has finished installing Crypta on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Finish

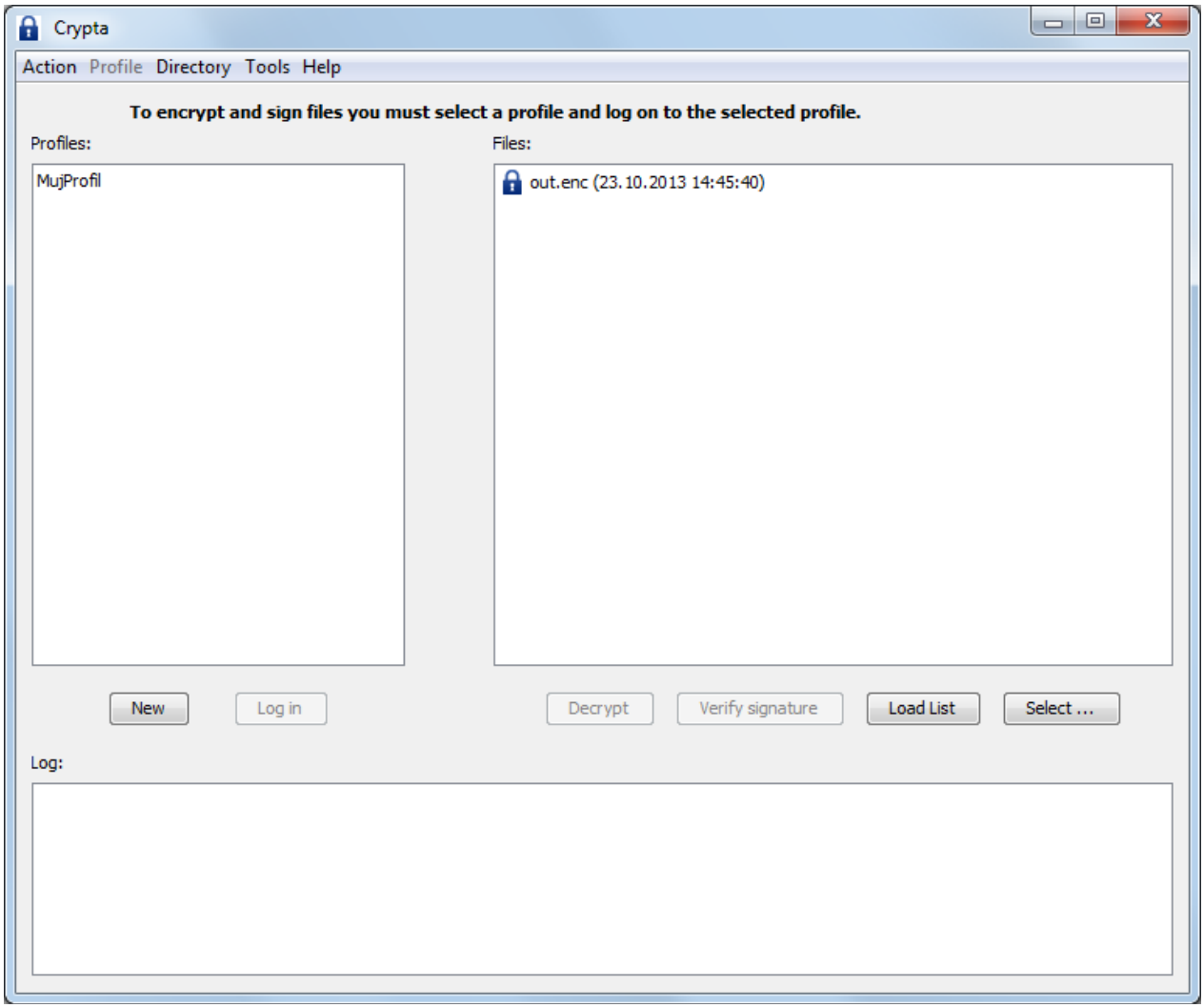
Chapter 4. Programme functions - without selected profile

4.1. Programme launch

In graphical regime, Crypta can be launched either by launching the Crypta.exe file for the Windows or Crypta for the Linux in the installation directory, or by the Crypta shortcut in the selected location.

The opening screen will display after the launch of the programme in graphical regime. You can select one of the actions offered by the menu or select one of the profiles or set up a new profile or select a file for decryption or signature verification. You can also change the configuration setting or use the help. The following paragraphs describe individual functions.

Picture 4.1. Opening screen



4.2. Application setting

You can access the application setting from the main menu by clicking on Tools/Application setting. The dialogue will offer you these directories:

- working directory, i.e. directory for storage of input and output files,
- directory with keys, i.e. directory for storage of files with profile keys,
- directory with partners' certificates,
- directory for storage of temporary files,
- directory for starage of CRLs,
- directory for storage of certificate application forms.

You can use the Select button to select the directory in the file system. The implicit setting refers to directories in the Crypta installation directory.

The application setting allows you to select a default size of the symmetric key for encryption according to the Advanced Encryption Standard (AESs), i.e. 128 or 256 bits.

The dialogue offers these options:

- Do not check the CRLs. This option is not implicitly set, it enables you to verify the signature if a current CRL is not available.
- Verify signature against the current time or against the signature time. The implicitly set option is verification against the current time. If you select verification against the signature time, you can verify a signature whose certificate is no longer valid.

The configuration allows you to set the HTTP proxy. Push the button Set proxy to display a dialogue for entry of the name or IP address of the proxy server and port ID#. If the access to the proxy server requires authentication, you can enter your user name and password.

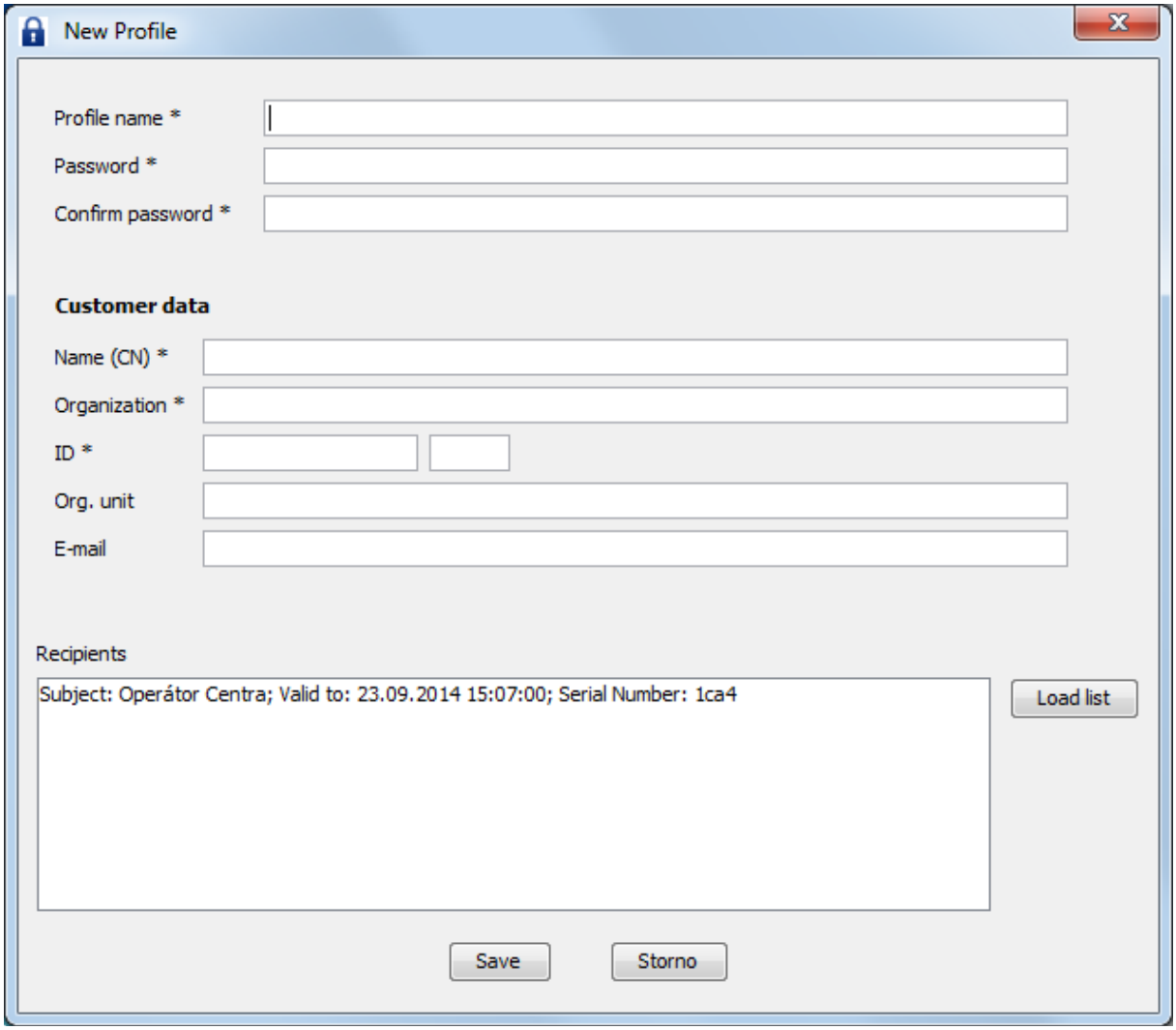
The application setting allows you to change the language in which texts including help are displayed. The default language is the language of the national environment of the operating system. The menu allows you to change the language to, e.g. English.

The Application setting dialogue displays the parameter values for communication with the PostSignum certification authority which cannot be edited here. These include:

- URL for sending online certificate renewal application form to PostSignum filing service,
- URL for submitting online certificate renewal application form to PostSignum filing service,
- URL for downloading certificates issued by the public certification authority PostSignum,
- URL for downloading CRLs issued by the public certification authority PostSignum.

Any changes recommended by Czech Post can only be made by editing the file jcrypta.properties in the application's installation directory.

Picture 4.2. Environment setting



Push the Save button to save the set values. Push the Cancel button to close the dialogue without saving the set values.

4.3. Ending programme

Select the option Action/End in the menu of the opening screen or the main screen of the profile to end the programme.

4.4. Adding profile

You need to create at least one profile to be able to start working with the programme. Push the New button in the opening screen to create a new profile. The New profile dialogue will display. Enter the obligatory name of profile and password in the upper section of the dialogue and confirm the password. In the Customer details section, enter the details which will be entered into the certificate:

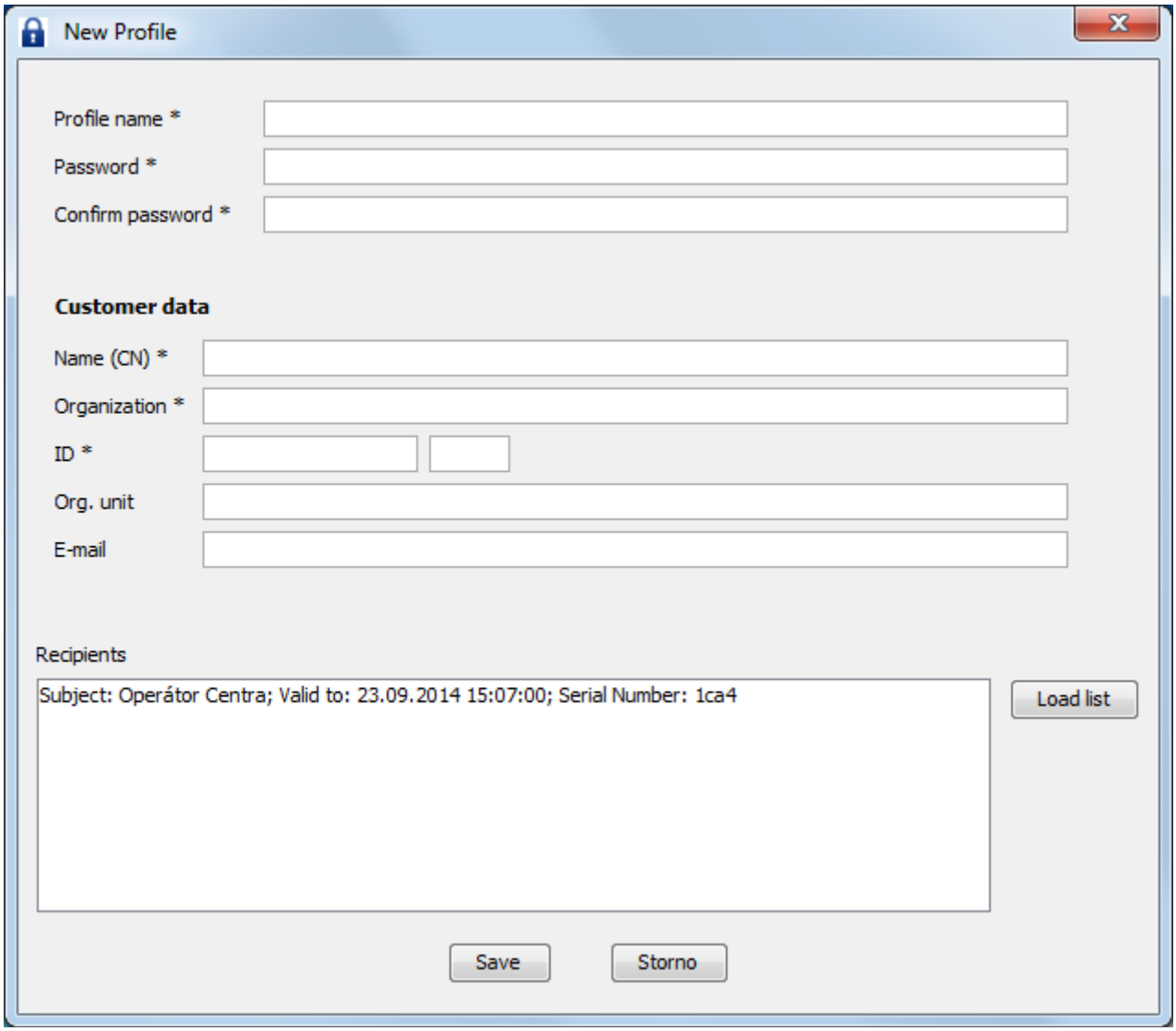
- Name (CN) - common name in the subject of the certificate, obligatory,
- Organisation - name of organisation, obligatory,

- ID# - identification number of organisation, obligatory,
- Organisational unit - optional,
- Email address - optional.

In the Recipients section, you can select the implicit profile recipient from the list of recipients. You can do so also later if the list of recipients is empty when you are setting up the profile. If you have changed the list of recipients while you are setting up the new profile, you can push the Read list button to update the list.

Push the Save button to save the profile with the entered values. Push the Cancel button to discontinue the dialogue.

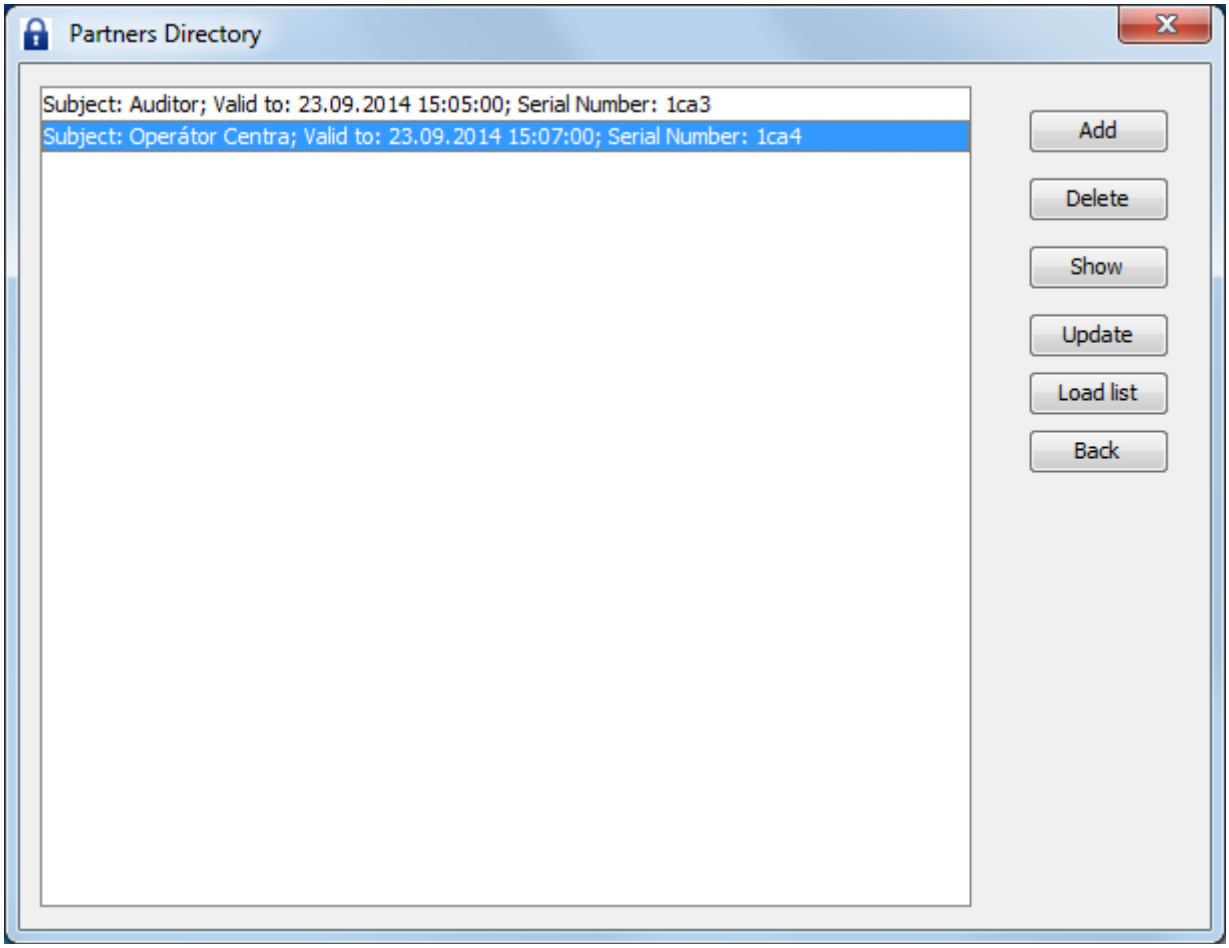
Picture 4.3. New profile



4.5. Partners directory

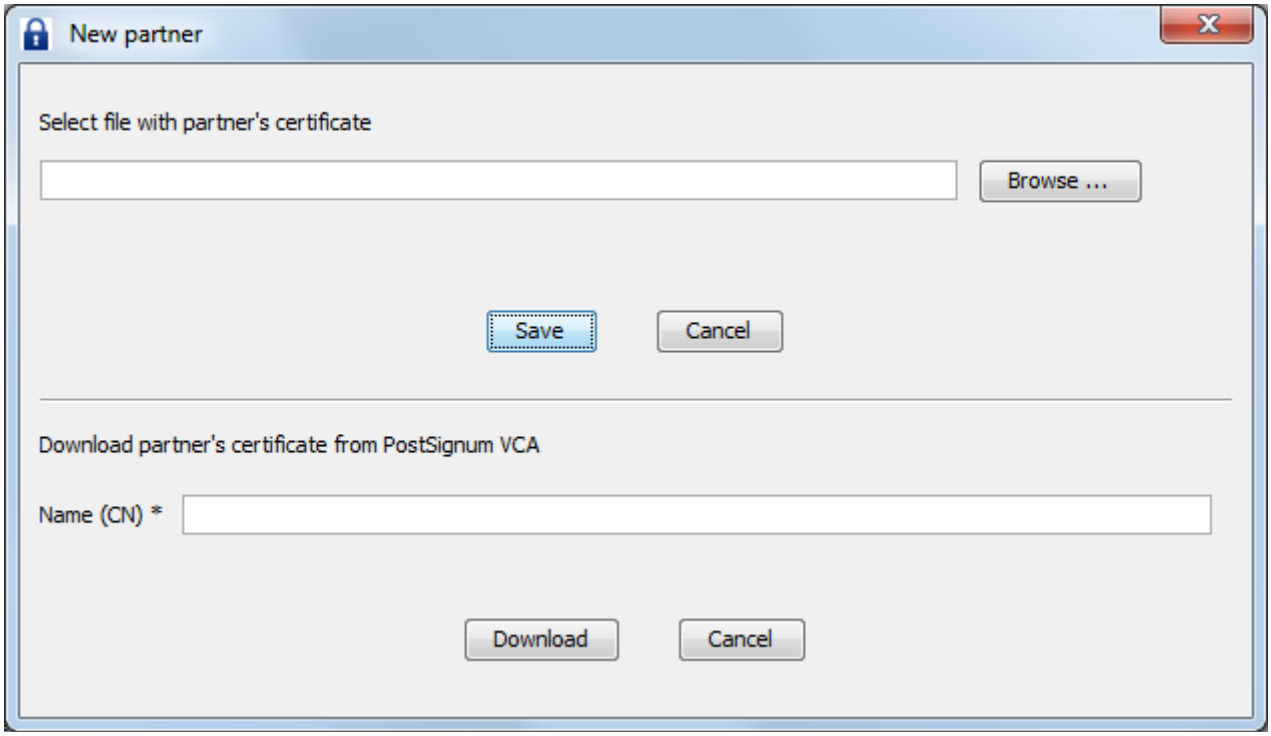
Crypta maintains a list of partners, i.e. potential recipients for whom encrypted files can be prepared. Select Directory in the main menu of the opening screen or the profile screen to display the form for partners management. The displayed details include common name from the subject of certificates of partners stored in the partners directory, certificate expiry date, and certificate serial number. You can select one of the actions in the right-hand column of the form, i.e. Add, Delete, View, Update, Read list, or push the Back button to discontinue the form.

Picture 4.4. Partners directory



The Add button - the New partner dialogue: You can set up a partner either by entering the file with his/her certificate or by entering the CN of his/her certificate which will then be automatically downloaded online via the public certification authority PostSignum services. Push the Delete button if you want to delete the recipient from the list.

Picture 4.5. New partner



Push the View button if you want a detailed summary of details in the recipient's certificate. Push the Update button to automatically download online from the PostSignum certification authority the certificate of the same issuer and holder with the longest validity. Push the Read list button to re-read the recipients from the data/certs directory.

4.6. Import of certificate

Select the option Tools/Import certificate in the main menu of the application's opening screen. A dialogue for selection of the file with certificate will display. The programme will compare the public key of the certificate with those of the profiles and if a matching key is found, a dialogue asking you to enter the password to the matching profile will display. The dialogue will contain the name of the found profile. Enter the password to launch the import. The main screen of the profile will display (same as when you log in to the profile) with the checked indication Certificate imported. An error message will display if the action fails or if invalid parameters are entered.

4.7. Update CRL

Select the Update CRL option to save the current CRL in the directory set in the configuration. The implicitly set directory for saving CRLs is _data/crls in the programme's installation directory. For instance, you can use another programme to download a CRL, select the Update CRL option to enter the CRL into the set directory, and continue to work with Crypta without network connection.

CRLs downloaded and used by Crypta for verification of certificates will not be stored by Crypta in the set directory. Files stored in the directory of CRLs must be contained in the directory already at the start of the programme, or you can use the Update CRL option to copy

them there additionally. Note: If the programme is already running, it is not enough to use the operating system tools to copy the CRL file into the set directory.

4.8. Error ouput

During communication with Czech Post support personnel you can be asked for sending in the error output file. Select the Tools/Error output option to create the file. The error.zip file is created in the programme's installation directory; it contains the log file log.txt and the file dir.txt with the content of the installation directory (names of files and directories). The error output file is to be sent by email.

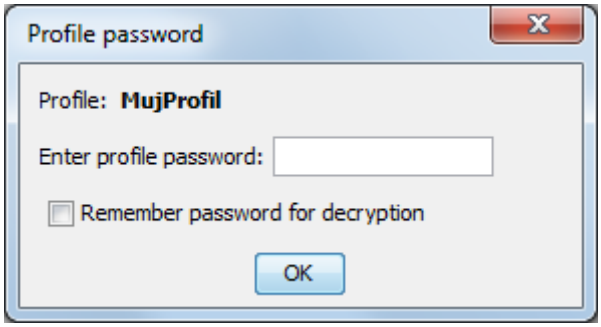
4.9. Decrypt

The decryption file is to be located in the working directory. You can then select the file in the opening screen menu and select Decrypt. Alternatively, you can click on the file name. The programme will find a suitable profile for decrypting the file and a dialogue asking you to enter the password to the profile will display. You can check the box for remembering the password for further decryption operations. The Decrypt dialogue follows. Because the decryption operation includes signature verification, the dialogue contains these options:

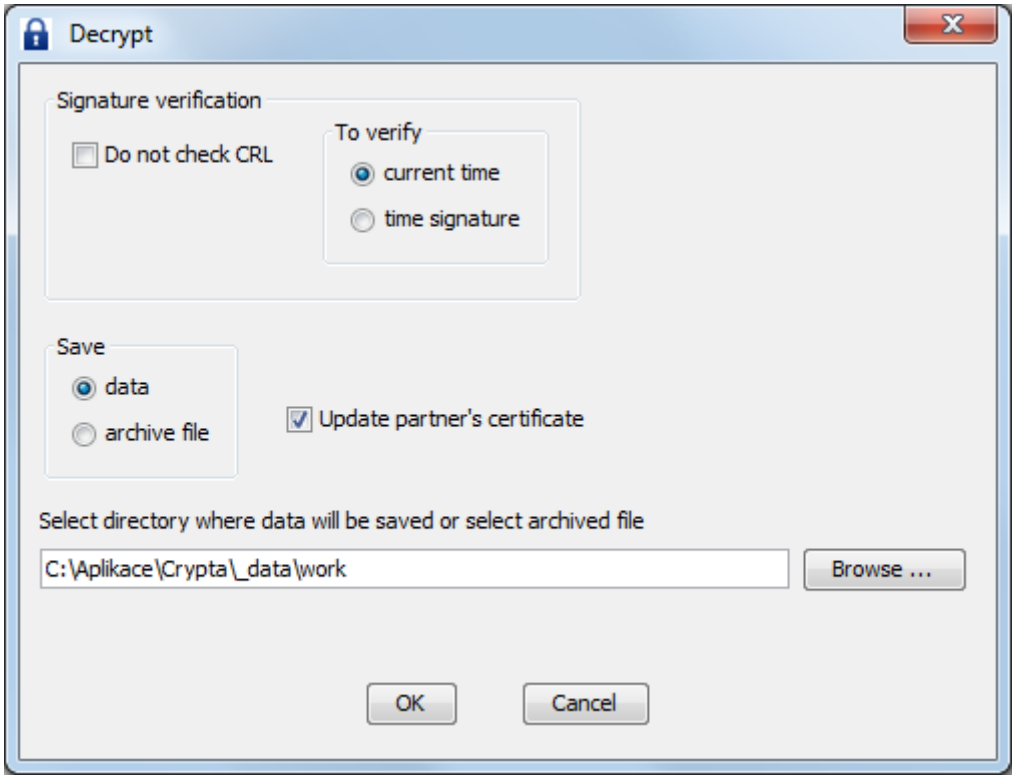
- Do not check CRLs. This option is not implicitly set, it enables you to verify the signature if a current CRL is not available.
- Verify signature against the current time or against the signature time. The implicitly set option is verification against the current time. If you select verification against the signature time, you can verify a signature whose certificate is no longer valid.

In the lower section of the dialogue, you can select the type of output, select whether it should be individual files, select the directory to store the files, or whether to sign the zip directory with the output. The dialogue contains a check box; if you check it, the partner's certificate from the signature in the file will replace the original certificate in the directory.

Picture 4.6. Enter profile password



Picture 4.7. Decrypt



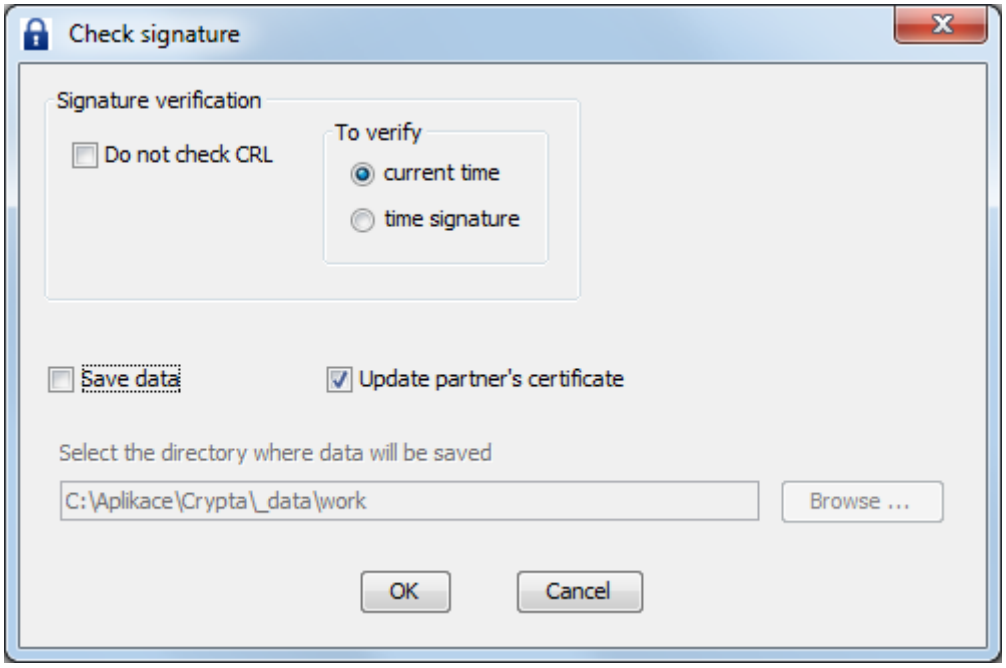
4.10. Verify signature

The file whose signature is to be verified must be located in the working directory. You can then select the file in the opening screen menu Files and select Verify signature. Alternatively, you can click on the file name. The dialogue Verify signature will display and you can set the operation. The dialogue again offers these options:

- Do not check CRLs. This option is not implicitly set, it enables you to verify the signature if a current CRL is not available.
- Verify signature against the current time or against the signature time. The implicitly set option is verification against the current time. If you select verification against the signature time, you can verify a signature whose certificate is no longer valid.

You can also select whether you only want to verify the signature in the archived file or store the data from the archived file in the directory. If you select the Save data option, a field for selection or entry of the directory in which the data is to be stored will display. If the selected directory already contains files with the same name, you will be asked whether the data is to be overwritten.

Picture 4.8. Verify signature



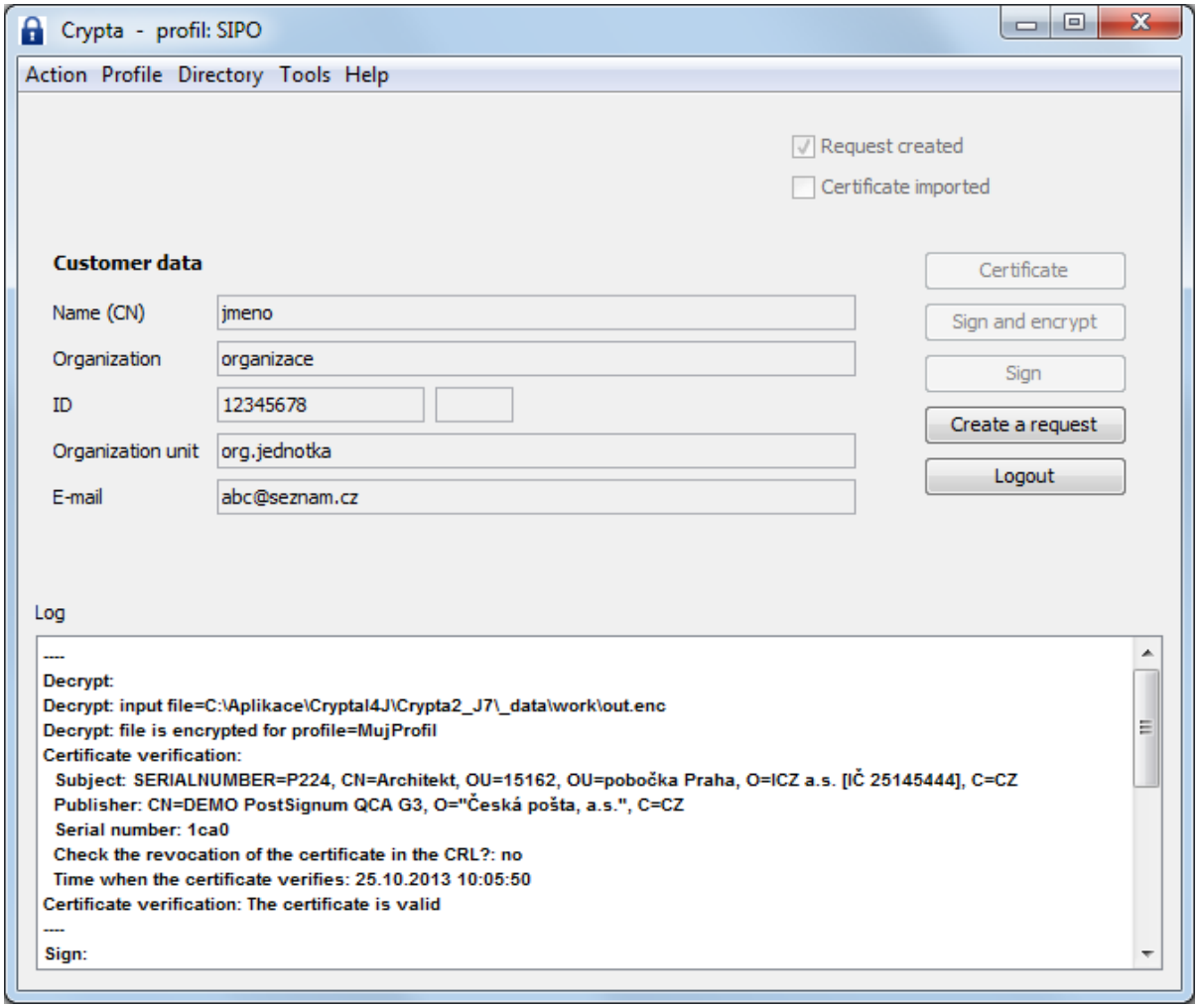
4.11. Profile login

Use the opening screen to log in to a profile. Select the profile in the Profiles window and continue with Login. Alternatively, you can click on the profile name. A dialogue asking you to enter the password follows. If the password is valid, the main screen of the profile will display. If the password is invalid, you will be informed and the programme will return to the opening screen.

Chapter 5. Programme functions - with selected profile

If you have selected a profile, the main screen of the profile will display. The displayed profile details are the customer details which are entered in the certificate, i.e. common name (CN), organisation (O), ID#, organisational unit (OU), and email address. The profile's main screen offers the following options for profile certificate management: generate application form, import certificate, export certificate, export pair of keys plus certificate (PKCS#12), import pair of keys plus certificate (PKCS#12).

Picture 5.1. Profile's main screen



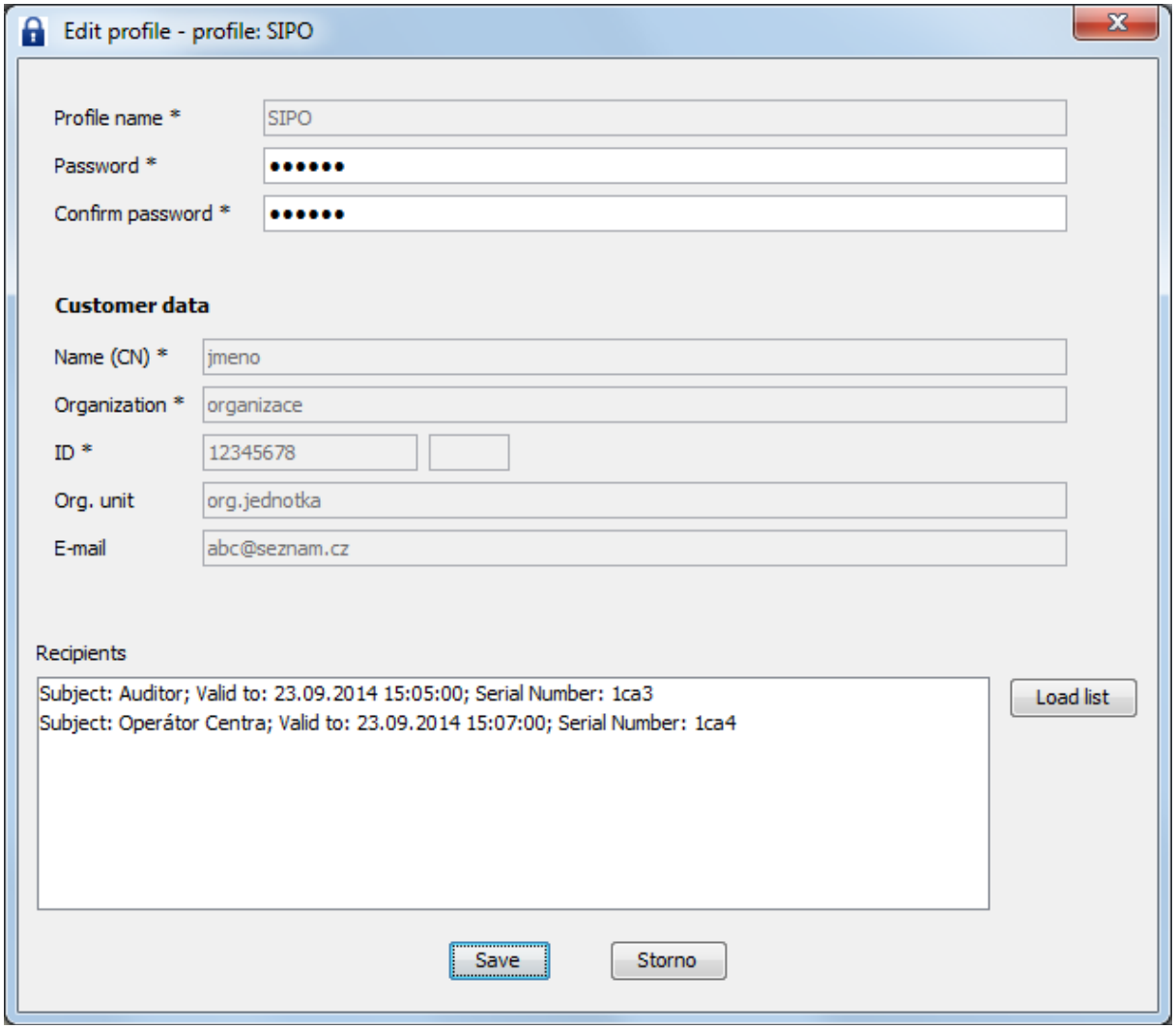
Unchangeable check boxes indicate whether an application form has already been generated and/or a certificate imported in the profile. If a certificate application form has been sent to the PostSignum applications storage facility, the application form's identification number will also display.

The right-hand section of the main screen of the profile contains the Sign and crypt and Sign buttons. You can use these buttons to display the below-mentioned dialogues. The menu on this screen contains the Edit profile and Application setting options.

5.1. Edit profile

Log in to the profile and select the Profile/Edit profile action in the main menu. You can use the Edit profile option to change the profile password and recipient settings only. Enter and confirm the new password. You will then be asked to authenticate your identity by entering the original password.

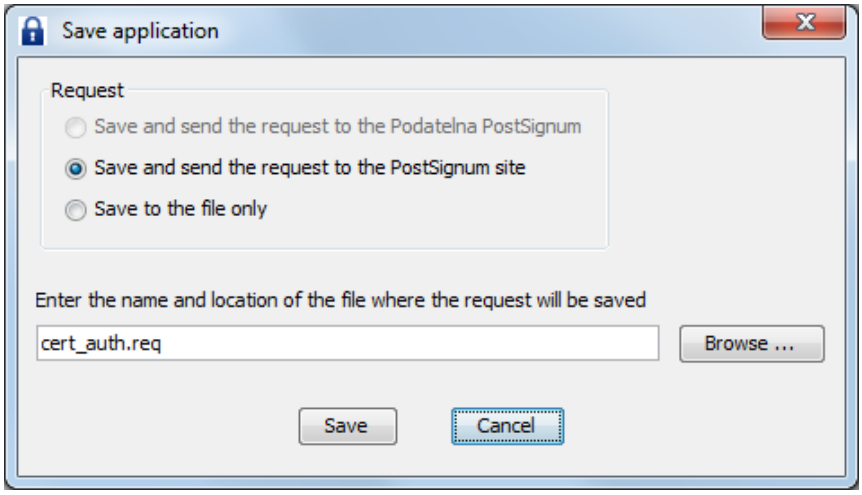
Picture 5.2. Edit profile



5.2.Generation of certificate application form

You can use the Generate application form option on the main screen of the profile to generate an application for certificate. This option can only be used if no certificate has already been imported into the profile. A dialogue asking you whether you want to save the file and offering you options for submitting the file. You can select the Save and submit application to the PostSignum website option or the Only save as file option and select the name and location of the file with the application form in the user system. The application form is saved in the PKCS#10 PEM format. The application form indication is then filled out in the profile. A log of actions made by the user is displayed in the lower section of the form. Once the certificate is issued, you can use the Tools/Import certificate option in the main menu of the programme's opening screen to import it.

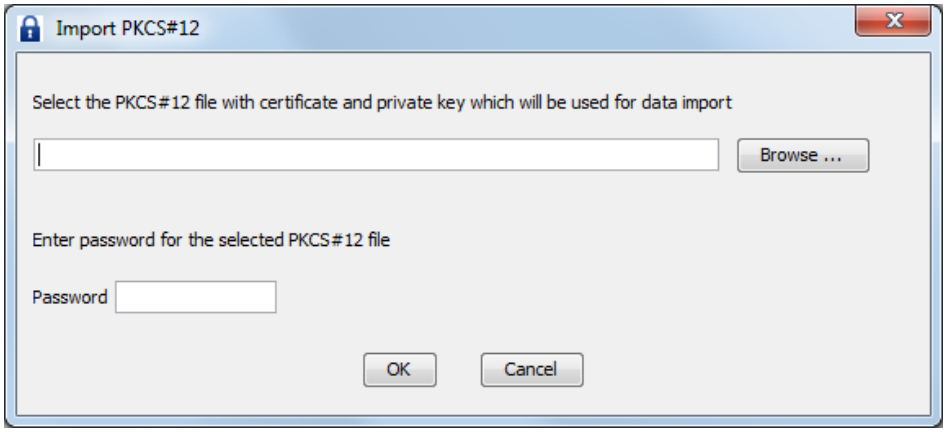
Picture 5.3. Save application form


Save application
Request
Save and send the request to the Podatelna PostSignum
Save and send the request to the PostSignum site
Save to the file only
Enter the name and location of the file where the request will be saved
cert_auth.req
Browse ...
Save
Cancel

5.4. Import pair of keys / PKCS#12

Select the Profile/Import PKCS#12 option to import a pair of keys. A dialogue for a new entry of the profile password will display. The password will be checked and a form for the selection of the PKCS#12 file and entry of its password will display. Enter the details to import a pair of keys and change the certificate identifier. A log of actions made by the user is displayed in the lower section of the form.

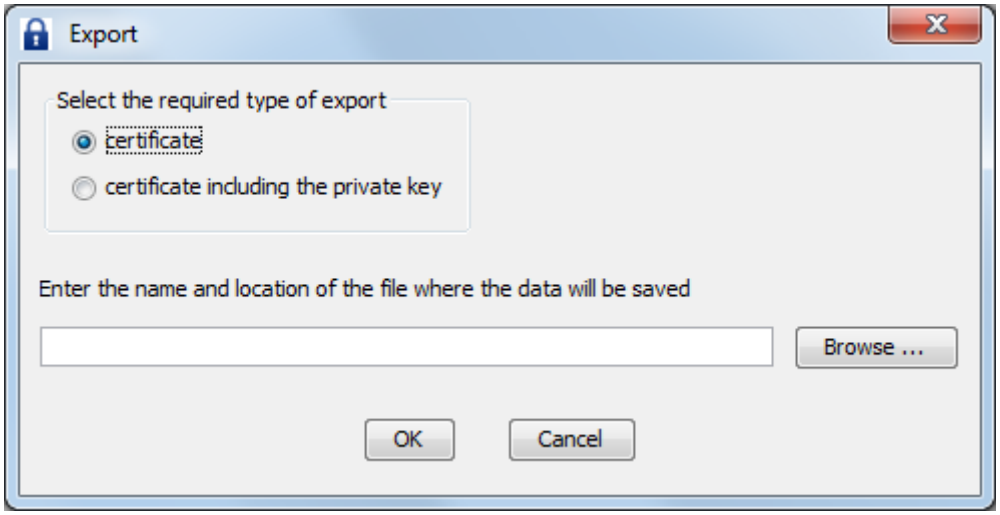
Picture 5.4. Import PKCS#12


Import PKCS#12
Select the PKCS#12 file with certificate and private key which will be used for data import
Browse ...
Enter password for the selected PKCS#12 file
Password
OK
Cancel

5.5. Export certificate and certificate including private key/PKCS#12

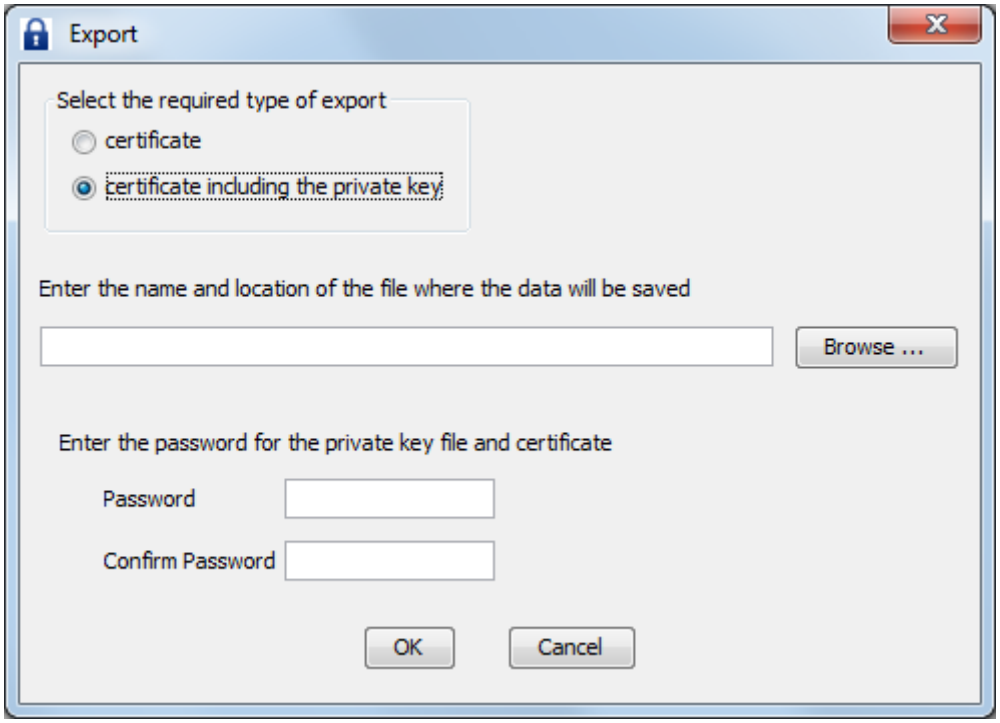
Use the Profile/Export certificate PKCS#12 option to export a certificate or pair of keys. A dialogue for export of certificate will display. The upper section of the dialogue contains selection of the type of export, whether the profile certificate is to be exported alone or including the private key. The export dialogue will change according to the selected option. If a certificate alone is to be exported, a field for entry of the export file will display. The implicit file suffix is cer. Once the file is selected, the certificate profile in the DER format will be exported. This option can only be used if the certificate has already been imported into the profile.

Picture 5.5. Export certificate



If a certificate including private key is to be exported, a dialogue asking you to enter the export file and password for PKCS#12 will display. The strength of the password will be checked. A dialogue asking you to enter the password for the profile will follow. After the entry of all valid details the export will be done.

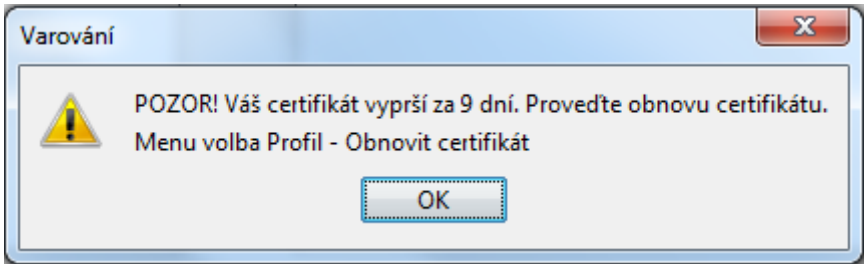
Picture 5.6. Export PKCS#12


Export
Select the required type of export
certificate
certificate including the private key
Enter the name and location of the file where the data will be saved
Browse ...
Enter the password for the private key file and certificate
Password
Confirm Password
OK
Cancel

5.6. Warning of upcoming certificate expiry

If a certificate is to expire in less than 20 days, the programme will warn you about the need for its renewal. The warning will display when you log in to the profile and during file decryption.

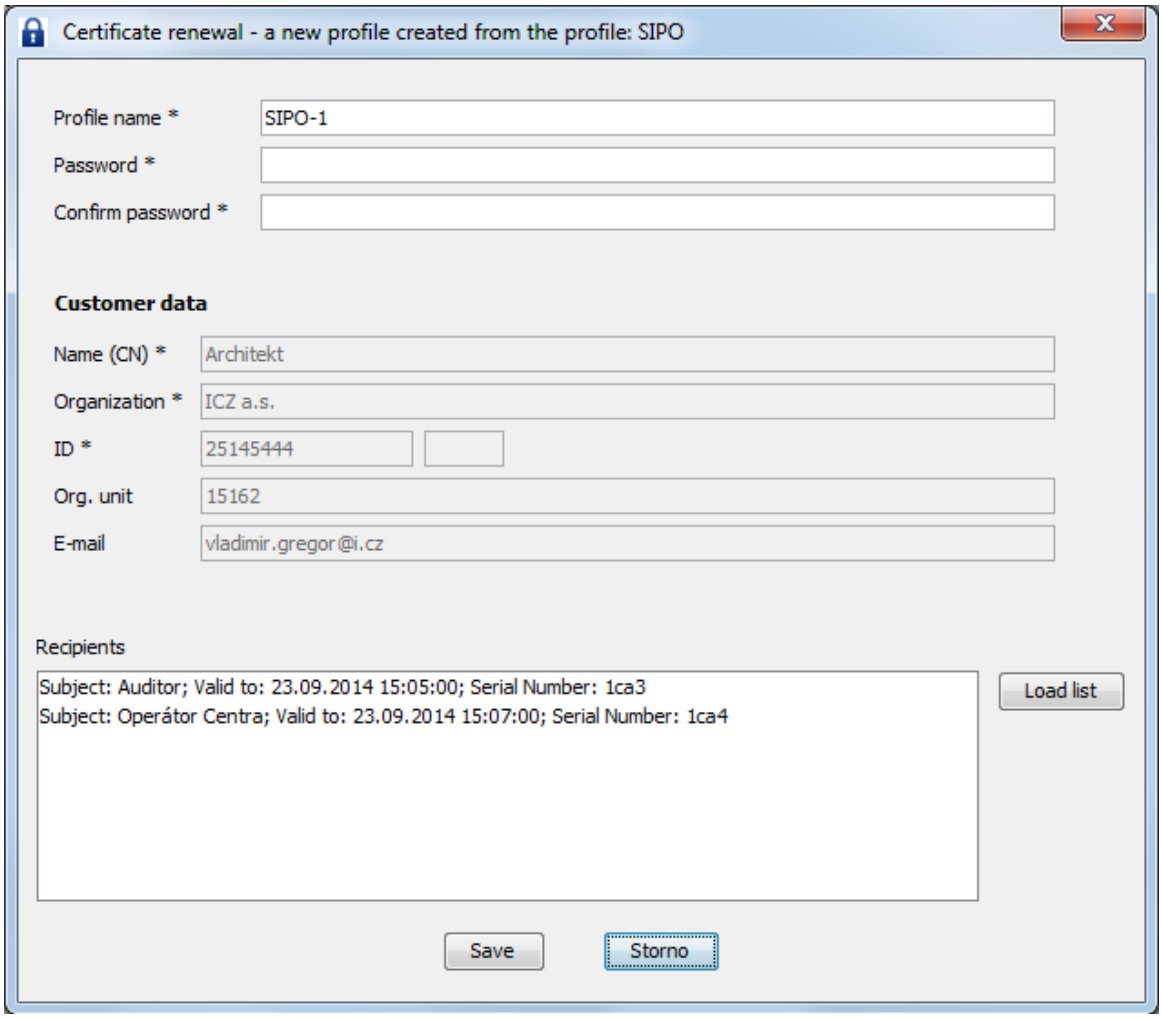
Picture 5.7. Warning of necessary certificate renewal



5.7. Certificate renewal

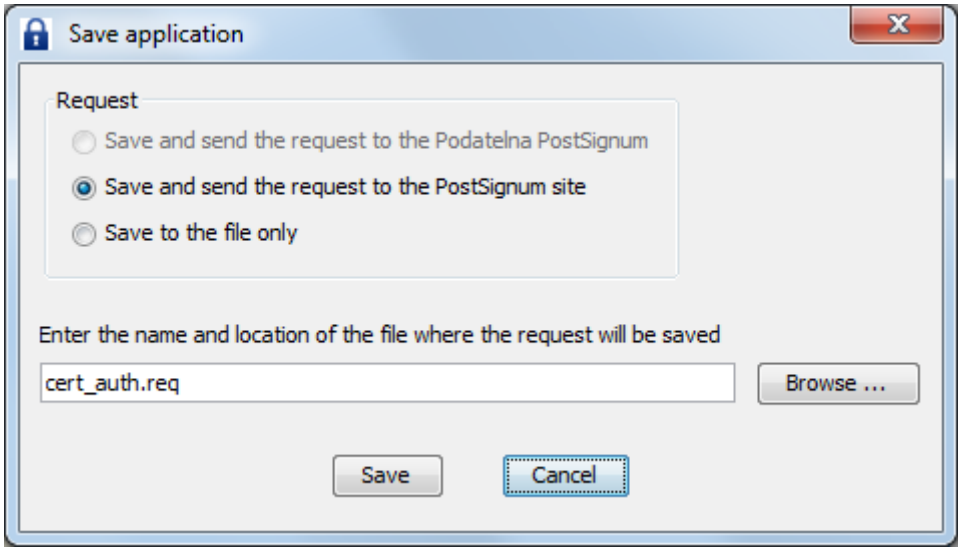
When a certificate is renewed, a new profile is generated as a copy of the original profile. You have to wait for the new profile to generate an application form for renewed certificate (certificate for the new profile). Log in to the profile and select the Profile/Renew profile action in the main menu. The new profile form containing details from the original certificate or profile will display. The value offered as the name of the new profile is the original profile name plus serial number. You can change the name of the new profile. You have to enter and confirm the password for the new profile.

Picture 5.8. Save and submit application form for renewed certificate



Once you have created a new profile, you can generate an application form and submit it to the PostSignum certification authority filing service. To do so, use the Save and submit renewal application form to PostSignum filing service in the Save application form dialogue. The data structure generated by the programme is signed with the key linked to the original certificate. The certification authority will issue so-called subsequent certificate and send you an email message with this information and instructions how to download the certificate.

Picture 5.9. Save and submit application form for renewed certificate


Save application
Request
Save and send the request to the Podatelna PostSignum
Save and send the request to the PostSignum site
Save to the file only
Enter the name and location of the file where the request will be saved
cert_auth.req
Browse ...
Save
Cancel

If the Save and submit renewal application form to PostSignum filing service option is not available, it means that the certificate you are trying to renew is no longer valid or has been revoked. In such case you can use the Save and submit application form to PostSignum website or Only save as file options.

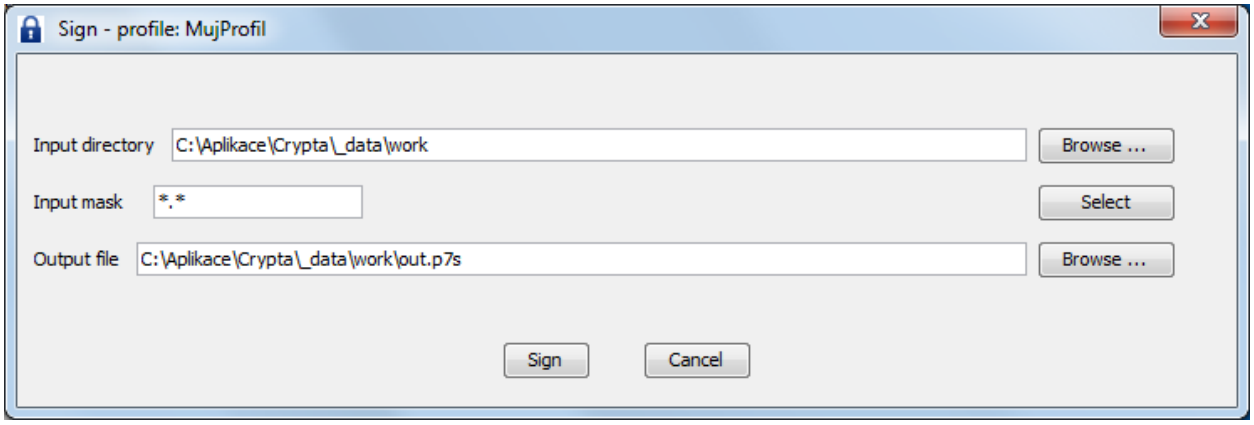
If you select the Save and submit application form to PostSignum website option, the form will be sent to the PostSignum certification authority website where it will be stored under the identification number which will be displayed to you. You must visit a Czech Post outlet offering CzechPoint services and show the counter clerk this number. If you select the Only save as file option, the application form will be saved as a file selected by you. You will have to produce the file containing the application form at a Czech Post outlet offering CzechPoint services.

Once the application form is generated and submitted, the new profile will indicate the existence of the application form in the profile. A log of actions made by the user is displayed in the lower section of the screen. Once the certificate is issued, you can use the Tools/Import certificate option in the main menu of the programme's opening screen to import it.

5.8. File signing

Log in to the profile and select the button Sign in the right-hand section of the profile's main screen. On the next screen, select the input data files, i.e. input directory and mask for selecting input files, output file name and location. Select the Sign button to confirm the action. The resulting file has the p7s suffix. A log of actions made by the user is displayed in the lower section of the profile's main screen.

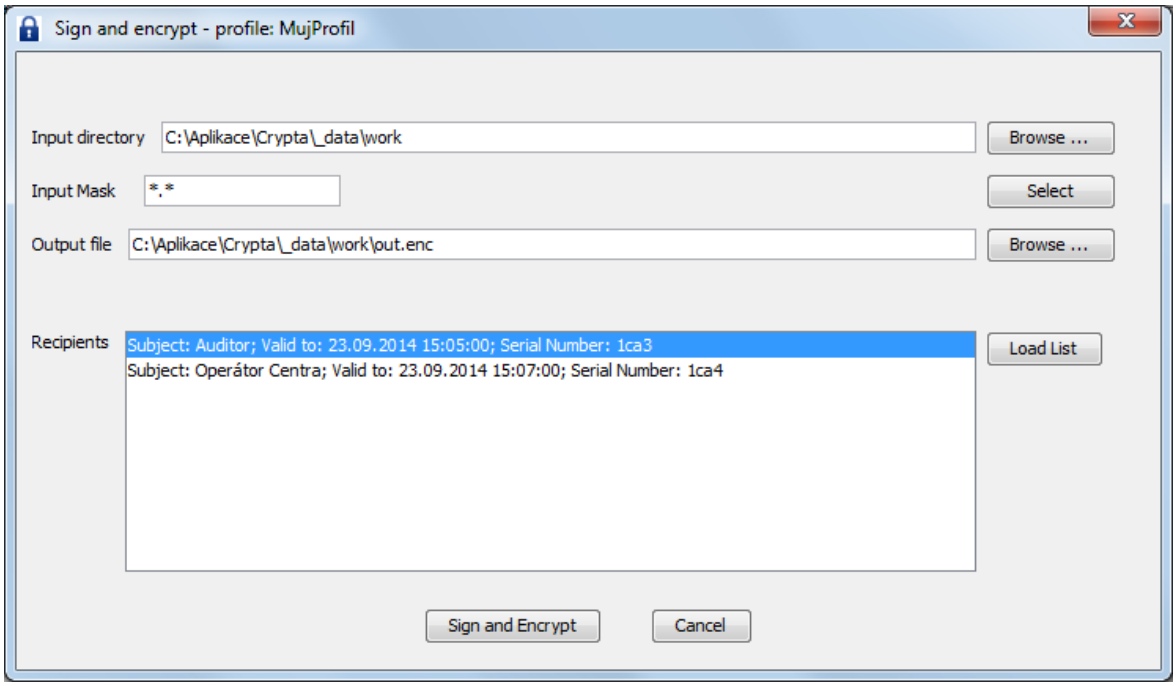
Picture 5.10. Sign



5.9. File signing and encrypting

Log in to the profile and select the button Sign in the right-hand section of the profile's main screen. On the next screen, select the input data files, i.e. input directory and mask for selecting input files, output file name and location, select addressees. Select the Sign and encrypt button to confirm the action. The selected files will be compressed, electronic signature of the compressed file will be generated, and the whole will be encrypted. The resulting file has the enc suffix. A log of actions made by the user is displayed in the lower section of the profile's main screen.

Picture 5.11. Sign and encrypt



Chapter 6. Unistallation

You can also use the installation programme if you want to uninstall Crypta.

Uninstallation procedure:

- Launch Unistall from the shortcut directory, or in the directory in which the client is installed launch the uninstall.exe file in the Windows or unistall in other systems.
- Select the Next button in the next window to confirm the action.
- After the uninstallation is finished, a window will display showing a list of files which were (intentionally) not uninstalled.
- Select the Finish bbutton to end the uninstaller.
- If necessary, back up the uninstalled files in another directory.
- The original directory in which the client was installed can now be deleted.

It is not recommended to use operating system tools to uninstall the programme, e.g. in the Windows do not use the option: Settings/Control panels/Add or remove programmes.

Appendix A. Command line interface

In the command line regime, use the CryptaCmd.exe or CryptaCmd.sh from the installation directory to launch the programme.

The command line interface design is based on the requirement of back compatibility with Crypta 1.3. Therefore all the existing switches (2,d,7,+,-) are allowed although they are ignored by the application. You can also enter the "e" and "s" parameters alone, without switches.

If a mask is used to enter input files, the path names must be enclosed in quotation marks. If a file with password is entered, it must be preceded with the character "?"; if a password is entered directly, it must be preceded with the character "!". If a password contains special characters, enclose the password in quotation marks.

Note for the MS Windows OS users: Use the normal rather than backslash character if you want to separate items in the path detail - see the examples for individual commands.

Note for the Linux OS users: If you enclose a password in quotation marks, use single marks. If you enclose the path to directories or files in quotation marks, enclose also the password in quotation marks. Example: '!Qq.1234'

1. Verification of certificates against CRLs in the command line regime

The way CRLs are used in the graphical regime is different from that in the command line regime. In the latter case, you must enter the valid CRL into the relevant directory according to the setting before you start working with it. To do so, use the commands for downloading or copying CRL as described in the following paragraphs. (If you use the graphical regime, you need not do this because the programme automatically downloads CRLs.)

2. Download CRL

You can download the current CRL from the public certification authority PostSignum's website and store it in the directory set for CRL storage, implicitly the _data/crls directory in the programme's installation directory.

```
CryptaCmd  ln crl
```

3. Copy CRL

You can copy the CRL file from its local position into the directory set for CRL storage, implicitly the _data/crls directory in the programme's installation directory. The command has a similar function as the Update CRL option in the graphical regime.

```
CryptaCmd cc file_name
```

Example:

```
CryptaCmd cc c:/import/vca2_crl.crl
```

4. Encryption

```
CryptaCmd e{2|d|7}{+|-} profile_name input_file output_file recipient_CN
{recipient_CN} {?file_with_password|!Password}
```

Example:

```
CryptaCmd e MyProfile "./in/*.pdf" ./out/vystup.enc recipient1 recipient2
?myPassword
```

Example:

```
CryptaCmd e MyProfile "./in/*.pdf" ./out/vystup.enc recipient1 !Qq.1234
```

5. Signing

```
CryptaCmd s{2|d|7}{+|-} profile_name input_file output_file
{?file_with_password|!password}
```

Example:

```
CryptaCmd s MyProfile "./in/*.pdf" ./out/vystup.p7s ?myPassword
```

9. Decryption

In the command line regime, you must enter the profile (name and password if required) for decryption.

```
CryptaCmd d profile_name input_file output_directory
{?file_with_password|!Password}
```

Example:

```
CryptaCmd d MyProfile ./prijem.enc ./open ?myPassword
```

Note: During decryption, a text file result.txt containing information about the decryption results is generated in the bin directory. If the decryption has been successful: "OK: sender_certificate_CN". If the decryption has failed: "Error: recipient_CN".

10. Archiving services,

```
CryptaCmd a profile_name input_file output_directory
{?file_with_password|!Password}
```

Example:

```
CryptaCmd a MyProfile ./prijem.enc ./archiv ?myPassword
```

11. Save password as file

```
CryptaCmd sp file_with_password
```

12. Certificate database content summary

```
CryptaCmd lcdb profile_name
```

13. Update recipient

Downloading the certificate with the given common name value which has the longest validity from the public certification authority PostSignum's server.

```
CryptaCmd  ln CN_atribut
```

Example:

```
CryptaCmd  ln "SIPO CENTRUM"
```

14. Check certificate status and validity

If the certificate exists and is available to download, the resulting details are: certificate CN, validity start and validity end dates. If the certificate is not available to download, the result will be return code 1 displayed on the screen.

```
CryptaCmd st CN_atribut
```

Example:

```
CryptaCmd  st "SIPO CENTRUM"
```

Appendix B. Application programme interface (API)

The Crypta API is described in a separate documentation as javadoc.